Sophicity

We put the IT in city

#CyberThreats

What?, How?, and Help!

Presenter

Dave Mims

CEO

davemims@sophicity.com
770-670-6940 x110

Sophicity
We put the IT in city

What we will cover

1. **What?** - What do I need to know?

2. **How?** – How have some real cities been impacted?

3. **Help!** – Where is help!

4. **Take Aways**

What?

What do I need to know?

- Passwords
- Virus Attacks
- Data Backup
- Security Updates
- Physical Security
- City Websites

Sophicity
We put the IT in city

What? - Passwords

A study from a research company in California found:

- 1 out of 3 people had their passwords written down somewhere around their desk.

- Many used obvious passwords (child name, pet name, college mascot, birthdate, etc).

- Overall, researchers figured out passwords of half of the people in the study!

I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."

Sophicity
We put the IT in city

What? - Passwords

SplashData’s annual **Worst Passwords List**, compiled from over 2 million **leaked** passwords during the year, shows people continue putting themselves at **risk**.

1. 123456	**2. Password**	**3. 12345678**	**4. qwerty**	**5. 12345**
6. 123456789	7. football	8. 1234	9. 1234567	10. baseball
11. welcome	12. 1234567890	13. abc123	14. 111111	15. 1qaz2wsx
16. dragon	17. master	18. monkey	19. letmein	20. login
21. princess	22. qwertyuiop	23. solo	24. passw0rd	25. starwars

Remember, hackers are using **automated software** to look for holes. That automated software attempts common and weak passwords that are easy to crack.

What? - Passwords

- Do not write passwords down and leave them visible
- Use a password on all devices (computer, laptop, tablet, phone, etc)
- Do not use obvious passwords. If your password is one from the top 25 worst passwords list, change it today!
- Use long passphrases or complex passwords consisting of a mix of letters, numbers, and special characters
- Do not save passwords to websites and applications
- Change passwords regularly
- Do not use the same password for all systems you access

Sophicity We put the IT in city

What? - Viruses

Computer viruses are **software programs** designed to spread and interfere. They will:

- **corrupt**, **delete**, and **steal** data
- use your access, email, social media, and messaging programs to **spread** itself
- hold your data hostage for **money** -- e.g. Ransomware!

Viruses can be disguised as attachments and links of, for example, funny images, greeting cards, online games, social media quizzes, or audio and video files.

What? - Viruses

- Install **business class antivirus software** on every computer (e.g. desktop, laptop, tablet, and phone!)
- Audit antivirus software regularly confirming installation and definitions are **up to date**.
- Train staff on common sources of viruses: **email attachments**, **websites**, and **online software**

People install viruses! We choose to download them. We trust too much.

What? – Data Backup

Ask yourself these questions:

- **Are** we backing up our data?
- **What** data is critical to the city? All of it?
- **How** will the city be affected if data cannot be accessed for extended periods of time?
- **Who** needs to be recovered first?
- **When** did we last test recovering our data?
- **Why** am I worried?

Sophicity
We put the IT in city

What? – Data Backup

- Perform onsite data backups of city data for **quick near recovery**. Time-to-recover should not be neglected.
- If the data is in question for backup, **back it up**.
- Perform offsite data backups to recover from **theft** or **disasters**.
- At a **minimum**, perform daily data backups.
- Ensure **no human** interaction is required.
- Have a plan for if there is a **disaster**.

Test your backups regularly! People choose to not test. We assume too much.

What? – Security Updates

Studies show:

- Most cyber outbreaks can be prevented by keeping computers **up to date**
- Applications (like Adobe Reader and Java) are **more likely** to be exploited than Operating Systems (like Windows)
- Most people **ignore** messages on their computers about installing updates

Sophicity
We put the IT in city

What? – Security Updates

- Let those updates and security patches **run!** Patch management is an essential element of cyber protection.
- As **vulnerabilities** are found, vendors create a fix and make a patch available, but those patches still have to be deployed.
- If you have servers, make sure an **IT resource** is updating them.
- Upgrade any application, operating system, and hardware that has reached **end of life**.

People ignore messages and warnings. We choose the risk. We are too impatient.

What? – Physical Security

Don’t forget the old-fashioned way of stealing

- Protecting city data also involves protecting **physical equipment**
- Theft or a **disgruntled employee** can be just as harmful as a hacked computer
- Decommissioned servers and workstations may still have **sensitive data** on them
- Most compromised networks occur from someone **internal**

Sophicity
We put the IT in city

What? – Physical Security

- **Lock computers** when away
- Ensure servers and network equipment are **locked up --** no direct access available
- Ensure external media (USB drives, backups, etc) are **locked up**
- Use **encryption** if possible
- Follow **password rules** identified earlier
- Have IT professionals **permanently and securely wipe** sunsetted equipment

People steal. We choose to allow access. We don't adequately secure our assets.

Sophicity
We put the IT in city

What? – City Websites

Today, when someone is interested in knowing more about your community, **where do they go first?**

And if your city website does not reflect your community well, **what do they do?**

- Is our city website **modern**?
- Is our city website's **content current**?
- Is our city website **secure**?

When did you personally last visit your city website? Could it be defaced and you **don't even know it**?

What? – City Websites

- Ensure the city website is hosted by a **reputable provider**
- Know **where** the city website is hosted
- Ask your website’s host if they have been **audited** for potential risks by a third party
- Follow **password rules** identified earlier

People judge quickly. We choose how to make the first impression. We are too quick to settle for just *good enough* when it isn’t really good enough.

How?

How have some real cities been impacted?

These are not **headlines** in the news. These are real cities and examples of what is seen **daily**. Cyber attacks are **costly**, **destructive**, & **embarrassing** for cities.

City #1: Virus initiates $90,000 transaction!

City #2: Virus deletes financial data!

City #3: Virus hacks city website!

Ransomware: Again!

Sophicity
We put the IT in city

How? – Virus $90K Xaction!

City #1: Real city that will remain anonymous.

- Finance officer gets a call from the city’s bank.
- A transaction in the amount of **$90,000** was just attempted from her computer.
- Her computer was compromised by a virus. The virus allowed her computer to be **remotely controlled** by an outside party.
- Finance officer panicked. **What do I do?**

How? – Financial data gone!

City #2: Real city that will remain anonymous.

- **Finance server** became infected with a virus.
- City’s data backup system **failed** to recover the data. **No one** had ever **tested** the backups!
- **Financial data lost**!

Data loss has **increased 400 percent** since 2012, while 71 percent of enterprises are not fully confident in their ability to recover after a disruption.

It's a great accounting program. Jenkins just downloaded it from deadlycomputervirus.com, sir.

Sophicity
We put the IT in city

How? – Website hacked!

City #3: Real city that will remain anonymous.

- **Citizens** visiting **the city's website** found nothing but advertisements. The website had been hacked and **all content replaced** with advertisements.
- The hacker **infiltrated** the **utility billing system** thru the online bill pay.

Citizen computers could have been infected with spyware/malware after visiting the city website. **Citizen information** may have been stolen.

Sophicity
We put the IT in city

How? – Ransomware again!

$$$

- A lot!
- Too often

The easiest way for a hacker to get in is when **someone lets them in** the door.

Sophicity
We put the IT in city

Help!

1. Legislative Audit
2. Top 10 Most Common Legislative Audit Issues
3. AML's IT in a Box
4. AML's IT in a Box drives Legislative Audit Compliance

Sophicity
We put the IT in city

Legislative Audit

Guidelines for **best practices and policies** to mitigate potential **information security risks.**

General Controls	Application Controls
• IS Management • Contract/Vendor Management • Network Security • Wireless Network Security • Physical Access Security • Logical Access Security • Disaster Recovery / Business Continuity	• Data Input • Data Processing • Data Output • Application Level General Controls

Top Legislative Audit Issues

Top 10

Top Legislative Audit Issues

10. **Physical Access Security** (risk: unauthorized access)

Top Legislative Audit Issues

10. **Physical Access Security** (risk: unauthorized access)

9. **Offsite Backups** (risk: data loss and inability to operate)

Top Legislative Audit Issues

10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)
8. **Audit Log not enabled** (risk: no insight into who or what XA)

Top Legislative Audit Issues

10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)
8. **Audit Log not enabled** (risk: no insight into who or what XA)
7. **Audit Log Report Review** (risk: missed errors/fraudulent XA)

Sophicity

We put the IT in city

Top Legislative Audit Issues

10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)
8. **Audit Log not enabled** (risk: no insight into who or what XA)
7. **Audit Log Report Review** (risk: missed errors/fraudulent XA)
6. **Disaster Recovery Planning** (risk: data loss, downtime, cost)

Sophicity
We put the IT in city

Top Legislative Audit Issues

10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)
8. **Audit Log not enabled** (risk: no insight into who or what XA)
7. **Audit Log Report Review** (risk: missed errors/fraudulent XA)
6. **Disaster Recovery Planning** (risk: data loss, downtime, cost)
5. **Wireless Access Policy** (risk: misuse or unauthorized access)

Sophicity
We put the IT in city

Top Legislative Audit Issues

10. **Physical Access Security** (risk: unauthorized access)

9. **Offsite Backups** (risk: data loss and inability to operate)

8. **Audit Log not enabled** (risk: no insight into who or what XA)

7. **Audit Log Report Review** (risk: missed errors/fraudulent XA)

6. **Disaster Recovery Planning** (risk: data loss, downtime, cost)

5. **Wireless Access Policy** (risk: misuse or unauthorized access)

4. **Passwords** (risk: unauthorized access)

Sophicity

We put the IT in city

Top Legislative Audit Issues

10. **Physical Access Security** (risk: unauthorized access)

9. **Offsite Backups** (risk: data loss and inability to operate)

8. **Audit Log not enabled** (risk: no insight into who or what XA)

7. **Audit Log Report Review** (risk: missed errors/fraudulent XA)

6. **Disaster Recovery Planning** (risk: data loss, downtime, cost)

5. **Wireless Access Policy** (risk: misuse or unauthorized access)

4. **Passwords** (risk: unauthorized access)

3. **Review Access Security** (risk: unauthorized access)

Sophicity
We put the IT in city

Top Legislative Audit Issues

10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)
8. **Audit Log not enabled** (risk: no insight into who or what XA)
7. **Audit Log Report Review** (risk: missed errors/fraudulent XA)
6. **Disaster Recovery Planning** (risk: data loss, downtime, cost)
5. **Wireless Access Policy** (risk: misuse or unauthorized access)
4. **Passwords** (risk: unauthorized access)
3. **Review Access Security** (risk: unauthorized access)
2. **Remote Access Policy** (risk: unauthorized access)

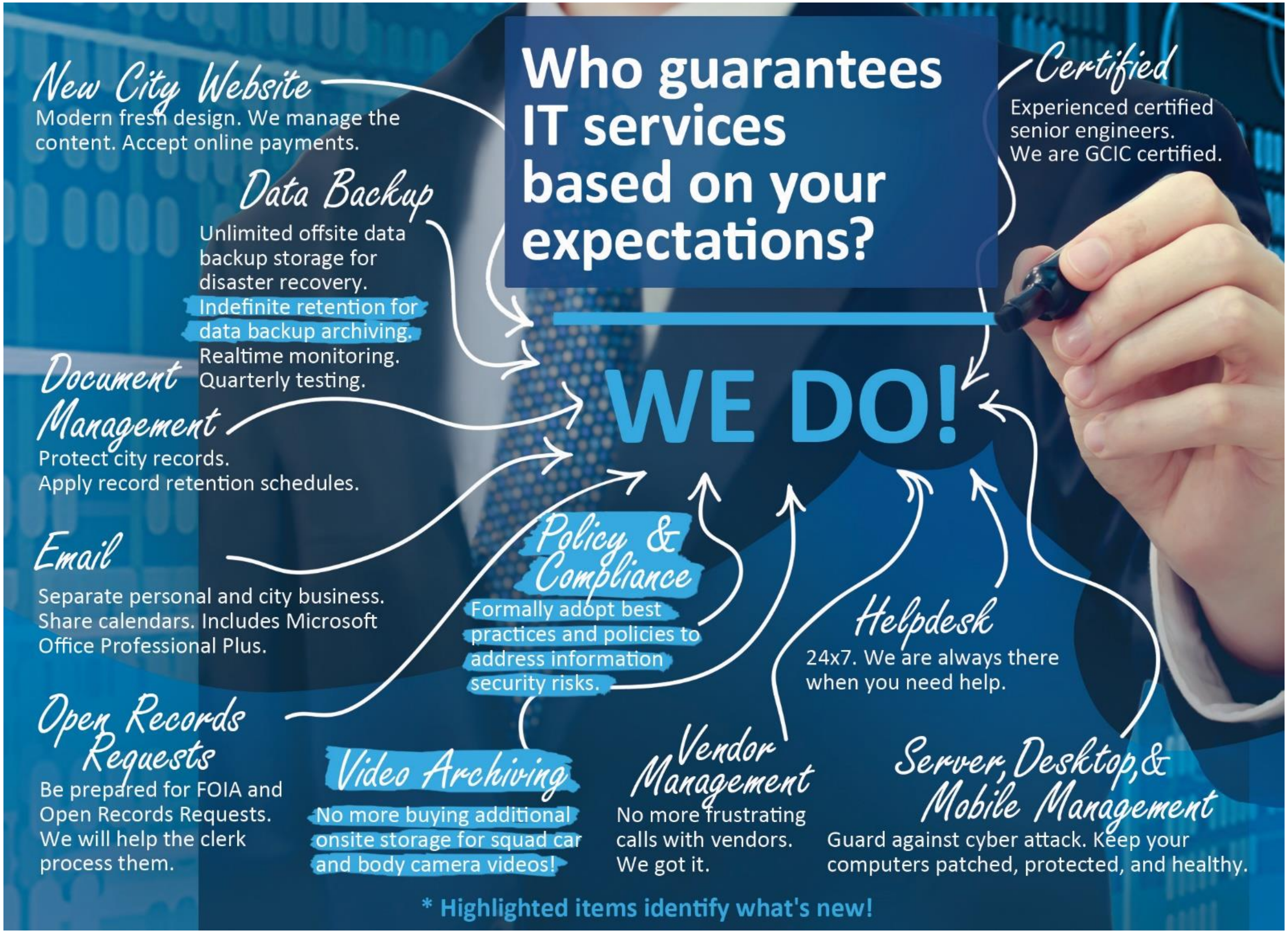
Sophicity
We put the IT in city

Top Legislative Audit Issues

10. **Physical Access Security** (risk: unauthorized access)
9. **Offsite Backups** (risk: data loss and inability to operate)
8. **Audit Log not enabled** (risk: no insight into who or what XA)
7. **Audit Log Report Review** (risk: missed errors/fraudulent XA)
6. **Disaster Recovery Planning** (risk: data loss, downtime, cost)
5. **Wireless Access Policy** (risk: misuse or unauthorized access)
4. **Passwords** (risk: unauthorized access)
3. **Review Access Security** (risk: unauthorized access)
2. **Remote Access Policy** (risk: unauthorized access)
1. **Data Integrity** (risk: data changes outside of process or approval)

Sophicity
We put the IT in city

AML's IT in a Box



Who guarantees IT services based on your expectations?

WE DO!

New City Website
Modern fresh design. We manage the content. Accept online payments.

Data Backup
Unlimited offsite data backup storage for disaster recovery.
Indefinite retention for data backup archiving.
Realtime monitoring.
Quarterly testing.

Document Management
Protect city records.
Apply record retention schedules.

Email
Separate personal and city business. Share calendars. Includes Microsoft Office Professional Plus.

Open Records Requests
Be prepared for FOIA and Open Records Requests. We will help the clerk process them.

Video Archiving
No more buying additional onsite storage for squad car and body camera videos!

Policy & Compliance
Formally adopt best practices and policies to address information security risks.

Vendor Management
No more frustrating calls with vendors. We got it.

Helpdesk
24x7. We are always there when you need help.

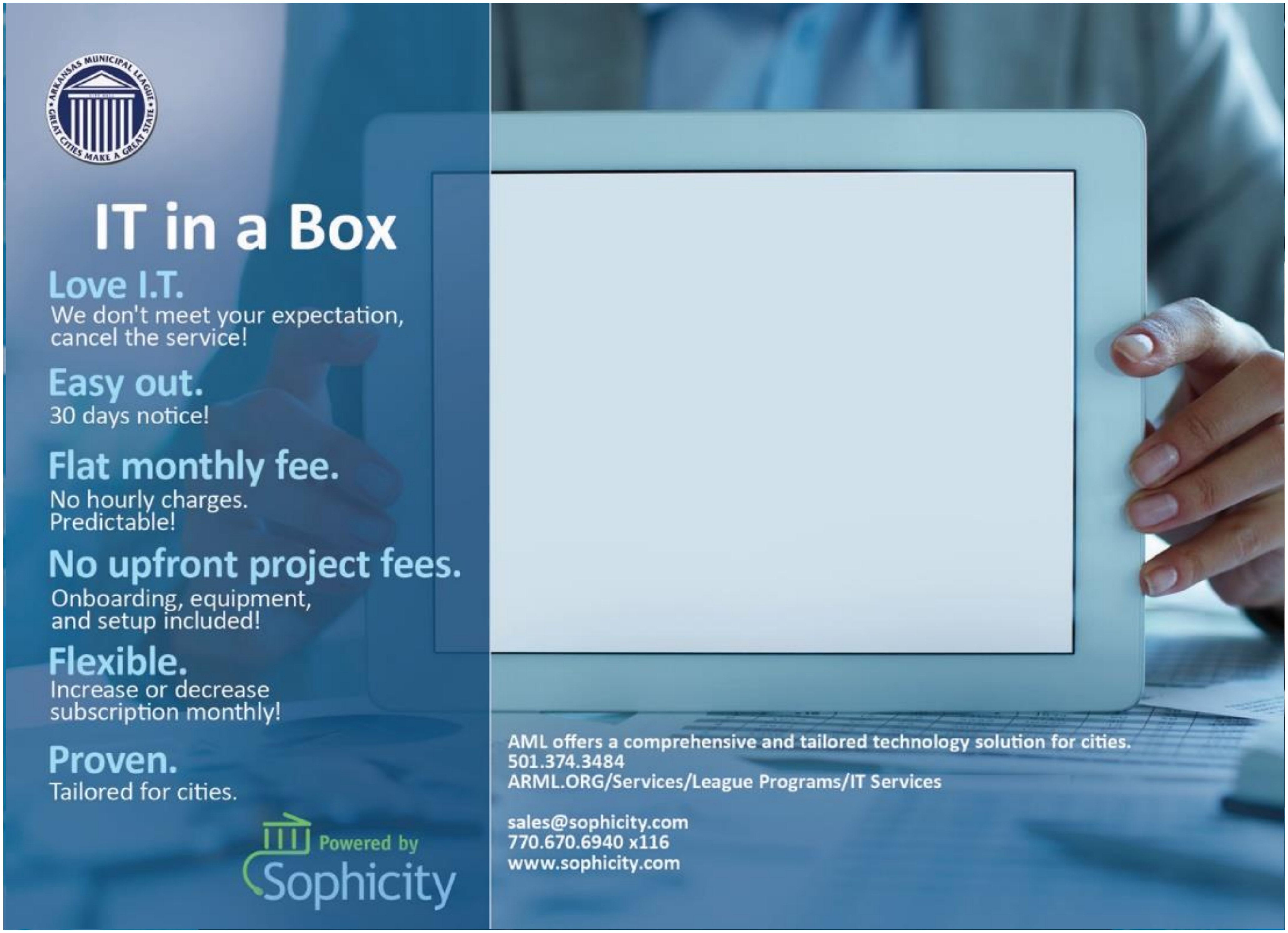
Server, Desktop, & Mobile Management
Guard against cyber attack. Keep your computers patched, protected, and healthy.

Certified
Experienced certified senior engineers. We are GCIC certified.

* Highlighted items identify what's new!

Sophicity
We put the IT in city

AML's IT in a Box



IT in a Box

Love I.T.
We don't meet your expectation, cancel the service!

Easy out.
30 days notice!

Flat monthly fee.
No hourly charges. Predictable!

No upfront project fees.
Onboarding, equipment, and setup included!

Flexible.
Increase or decrease subscription monthly!

Proven.
Tailored for cities.

Powered by Sophicity

AML offers a comprehensive and tailored technology solution for cities.
501.374.3484
ARML.ORG/Services/League Programs/IT Services

sales@sophicity.com
770.670.6940 x116
www.sophicity.com

Sophicity
We put the IT in city

Drive Leg Audit Compliance

AML's IT in a Box provides a **comprehensive** stack of technologies and services **tailored** to cities meeting federal, state, and local government **compliance**.

Drive Leg Audit Compliance

AML's IT in a Box provides a **comprehensive** stack of technologies and services **tailored** to cities meeting federal, state, and local government **compliance**.

1. **Scorecard** provides compliance roadmap and measures compliance status.

Sophicity
We put the IT in city

Drive Leg Audit Compliance

AML's IT in a Box provides a **comprehensive** stack of technologies and services **tailored** to cities meeting federal, state, and local government **compliance**.

1. **Scorecard** provides compliance roadmap and measures compliance status.

2. **Technical Account Managers** drive all parties (city, vendors, auditors, and engineering staff) to complete scorecard requirements.

Sophicity

We put the IT in city

Drive Leg Audit Compliance

AML's IT in a Box provides a **comprehensive** stack of technologies and services **tailored** to cities meeting federal, state, and local government **compliance**.

1. **Scorecard** provides compliance roadmap and measures compliance status.
2. **Technical Account Managers** drive all parties (city, vendors, auditors, and engineering staff) to complete scorecard requirements.
3. **Policies** are adopted. Technologies are deployed. Processes are implemented. Stabilization occurs. Compliance is reached. I.T. Operations Manual compiled.

Sophicity
We put the IT in city

Drive Leg Audit Compliance

AML's IT in a Box provides a **comprehensive** stack of technologies and services **tailored** to cities meeting federal, state, and local government **compliance**.

1. **Scorecard** provides compliance roadmap and measures compliance status.

2. **Technical Account Managers** drive all parties (city, vendors, auditors, and engineering staff) to complete scorecard requirements.

3. **Policies** are adopted. Technologies are deployed. Processes are implemented. Stabilization occurs. Compliance is reached. I.T. Operations Manual compiled.

4. **Manage** ongoing. **Test** regularly. **Adapt** as technology changes.

Sophicity
We put the IT in city

Recap

What? – We've covered 'What you need to know'?

How? – We've covered 'How some real cities have been impacted'?

Help! – We've covered 'Help from Legislative Audit and AML's IT in a Box'!

Know cyber crimes affect all cities, not just big ones.

Don't be an easy target. Don't be a victim. Don't be headline news. -- Take action! Be proactive!

Take Aways

- Is our **city** at risk?
  - Cyber attack? Records/Data loss? Unauthorized Access (external or internal)? Erroneous changes? Website?

Take Aways

- Is our **city** at risk?
  - Cyber attack? Records/Data loss? Unauthorized Access (external or internal)? Erroneous changes? Website?
- Is our **technology** dated?
  - Unlicensed? Unsupported? No longer maintained? Still using paper?

Sophicity
We put the IT in city

Take Aways

- Is our **city** at risk?
  - Cyber attack? Records/Data loss? Unauthorized Access (external or internal)? Erroneous changes? Website?
- Is our **technology** dated?
  - Unlicensed? Unsupported? No longer maintained? Still using paper?
- **Frustrated** with anything I.T.? Or, even all things I.T.?

Sophicity
We put the IT in city

Take Aways

- Is our **city** at risk?
  - Cyber attack? Records/Data loss? Unauthorized Access (external or internal)? Erroneous changes? Website?
- Is our **technology** dated?
  - Unlicensed? Unsupported? No longer maintained? Still using paper?
- **Frustrated** with anything I.T.? Or, even all things I.T.?
- Unable to meet **Legislative Audit compliance**?

Sophicity
We put the IT in city

Take Aways

- Is our **city** at risk?
  - Cyber attack? Records/Data loss? Unauthorized Access (external or internal)? Erroneous changes? Website?
- Is our **technology** dated?
  - Unlicensed? Unsupported? No longer maintained? Still using paper?
- **Frustrated** with anything I.T.? Or, even all things I.T.?
- Unable to meet **Legislative Audit compliance**?

When you subscribe to **AML's IT in a Box:**

☑ Cyber protection is provided & proactively managed
☑ I.T. needs are addressed & proactively kept modern
☑ Legislative Audit compliance is met & proactively maintained

Sophicity
We put the IT in city

I’m here all conference…

Dave Mims, CEO
davemims@sophicity.com
770-670-6940 x110

Visit us on the web at:
Sophicity.com

Sign up for our Monthly Newsletter

Sophicity
We put the IT in city

Take Aways

We have **blogged** extensively on these topics at **Sophicity.com**, so leverage these **weekly** *to-the-point* and *in-plain-English* articles to bring **awareness** of the risks to your **staff**:

- Patch Management: A boring task that prevent scary threats
- 5 Reasons Your City is an Easy Target for Hackers
- Why Hackers' Jobs Got Even Easier in 2015
- Don’t Decommission Hardware Yourself—Call the Professionals
- Preparing for Cyberattacks in a Dangerous World
- You're Backing Up Your Data, But Can You Recover It?
- 5 Tips to Tackle Information Security from the Inside
- 5 Ways to Stop Hackers from Stealing Your City's Most Sensitive Data
- 5 Tips to Help Employees Avoid Clicking on Malicious Emails
- Why Is My Small City Considered a Cybersecurity Threat? Here's Why

…

Sophicity
We put the IT in city